Notice of Allowability	Application No.	Applicant(s)	
	09/878,320	CROSBIE ET AL.	
	Examiner	Art Unit	
	Pramila Parthasarathy	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *10/25/2005*.

2. ☒ The allowed claim(s) is/are *1-12, 14, 16-19, 21,26, Renumbered as Claims 1-19*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

DETAILED ACTION

Claim Rejections - 35 USC § 112

1. The rejection of Claims 1 – 12, 14, 16 – 18, 21 and 26 under 35 U.S.C. 112, second paragraph has been withdrawn.

Allowable Subject Matter

2. Claims 1 – 12, 14, 16 – 19, 21 and 26 are allowed.

3. The following is an examiner's statement of reasons for allowance: The Admitted prior art Moran U.S. Patent 6,647,400, hereafter "Moran", disclose an intrusion detection system comprising an analysis engine configured to apply forward- and backward-chaining using rules from the source of rules, where the rules configure the system to collect, correlate, and evaluate data related to all phases of an attack, enabling detection of attacks involving novel (unknown) components and attacks where all evidence of one or more components is missing.

Moran further discloses an intrusion detection system comprising a mechanism for checking timestamps, configured to identify backward and forward time steps in a log file, filter out expected time steps, correlate them with other events, compares the timestamps of a directory and its files and identifies values that are inconsistent or not accounted for, and assigns a suspicion value to the associated file or directory.

However, the admitted prior art does not disclose, teach or suggest "parsing means for parsing the records and comparing the parsed records against one or more templates using an event driven correlation, wherein the event driven correlation uses an Event Correlation Services (ECS) engine core".

The present invention provides an Event Correlation Services (ECS) for the correlation of discrete events over time and the ECS engine is embedded within the IDS correlator process to improve performance, to parse and understand kernel audit records, system log files and other data source by using a meta-description language for fast parsing of the event streams.

5. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

6. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Randy A. Noranbrock, registration number 42,940 on November 02, 2005.

IN THE CLAIMS:

1. (Amended) A computer architecture for an intrusion detection system, comprising:

a control agent to interface with a management system and to monitor system activity;

at least one data gathering component which gathers kernel audit data and syslog data;

at least one correlator to interpret and analyzes the kernel audit data and the syslog data using at least one detection template,

wherein said at least one correlator uses an event driven correlation using an Event Correlation Services (ECS) engine core,

wherein said at least one detection template is selected from the group including:

a modification of files/directories template;

a chance to log files template;

a SetUID files template;

a creation of world-writables template;

a repeated failed logins template;

a repeated failed SU commands template;

a race conditions attack template;

a buffer overflow attacks template;

a modification of another user's file template;

a monitor for the start of interactive sessions template; and

a monitor logins/logouts template.

5. (Amended) The computer architecture of claim 4, further comprising a communication agent which encrypts information sent from said intrusion detection system to said management ~~station~~ system.

8. (Amended) The computer architecture of claim 6 , wherein said high bandwidth connection is used to send and receive memory-mapped files.

19. (Amended) A computer architecture for detecting intrusions, comprising:

reading means for reading kernel records;

reformatting means for reformatting each of the read kernel records into a different format;

parsing means for parsing the records and comparing the parsed records against one or more templates using an event driven correlation. wherein the event driven correlation uses an Event Correlation Services (ECS) engine core, wherein the at least one template is selected from the group including:

a modification of files/directories template;

a chance to log files template;

a SetUID files template;

a creation of world-writables template;

a repeated failed logins templates;

a repeated failed SU commands template;

a race conditions attack template;

a buffer overflow attacks templates;

a modification of another user's file templates;

a monitor for the start of interactive sessions template; and

a monitor logins/logouts template.

21. (Amended) A computer system, comprising:

a processor; and

a memory coupled to said processor, the memory having stored therein sequences of instructions, which, when executed by said processor, causes said processor to perform the steps of

reading means for reading kernel records;

reformatting means for reformatting each of the read kernel records into a different format;

parsing means for parsing the records and comparing the parsed records against one or more templates using an event driven correlation,

wherein the at least one template is selected from the group including:

a modification of files/directories template;

a chance to log files template;

a SetUID files template;

a creation of world-writables template;

a repeated failed logins templates;

a repeated failed SU commands template;

a race conditions attack template;

a buffer overflow attacks templates;

a modification of another user's file templates;

a monitor for the start of interactive sessions template; and

a monitor logins/logouts template,

wherein said event driven correlation uses an Event Correlation Services (ECS) engine core.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Pramila Parthasarathy whose telephone number is 571-272-3866. The examiner can normally be reached on Tuesday – Thursday 8:00a.m. To 3:00p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-232-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR only. For more information about the PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Pramila Parthasarathy
November 02, 2005.

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100